December 2001 *Issues Paper 13-01*

DEFENDING THE DEFENDER
KEEPING THE SHIELD STRONG

By Professor Michael Pasquarett, Colonel Patrick Carney, Colonel Peter Cohen, and Colonel Richard Dillon

INTRODUCTION

If, or more likely ***when***, the United States begins to construct and field a viable missile defense system, those who oppose this country's aims will most likely also begin to craft a response. What types of responses will they chose? We can be sure they will take measures intended to overcome or at least reduce the effectiveness of any type of missile defense system the United States decides to employ. While there has been extensive discussion of possible offensive missile countermeasures (decoys, warhead shielding, quantitative overmatch, etc.), there appears to have been less consideration given to the possibility that an opponent might choose some method of direct attack on the infrastructure of the missile defense system itself. However, some adversaries already may be focusing on asymmetric methods to attack United States missile defense capabilities rather than engage in a major offensive missile buildup necessary to directly challenge an American missile defense system.

If this is true, how do we protect our missile defense system from such attack, particularly from non-missile attacks? A recently conducted workshop at the U. S. Army War College's Center for Strategic Leadership examined this issue.

Over thirty-five subject matter experts from both the federal government and the private sector participated in the three-day workshop conducted at the U.S. Army War College's Collins Center from 26-28 November 2001. The purpose of the workshop was to explore issues regarding the security of our present and future space and missile defense systems, especially from asymmetric threats. Workshop participants examined the vulnerabilities of the National Missile Defense (NMD) and Theater Missile Defense (TMD) portions of the Integrated Missile Defense (IMD) system based on projected operational concepts briefed during the workshop.

Three distinguished speakers began the workshop with presentations addressing a multitude of potential threats to and vulnerabilities of projected United States' missile defense systems. LTG

Edward G. Anderson III, Deputy Commander in Chief, United States Space Command, during both his keynote address and an early workshop session presentation provided the national and joint perspectives on space and missile defense. Subsequently discussed were a full range of protective measures that might be employed to improve the survivability of United States missile defenses.

Within this context, the workshop focused on identifying specific major vulnerabilities of the United State's IMD shield, and suggested measures that could be developed to safeguard our missile defense systems and improve their security both at home and abroad. Workshop participants were divided into four groups, two each for America and Overseas. Each group developed a unique threat attack plan and subsequently proposed countermeasures to their own and the other groups' threats. The workshop addressed three phases of IMD deployment/employment: Phase I, from decision to deploy through deployment of initial operating capabilities (IOC); Phase II, from IOC deployment through enemy's decision of engagement in a hot war; Phase III, from an enemy's decision to engage in open war through conclusion of the conflict.

GROUP DISCUSSIONS

PHASE 1: Development Through Initial Operating Capabilities (IOC)

Participants generally agreed that threat actions would include a synchronized, integrated, and sustained campaign to discourage United States development and deployment of IMD systems. A main focus of this threat program would be the "will of the people." Adversaries clearly understand that by negatively influencing Americans on the potential failures of the systems, costs in both treasure and world public opinion, and even the overall need for such a defensive system can cause such programs to be delayed or even cancelled. In this regard, Executive Branch oversight measures are recommended to ensure a comprehensive federal, state, local and multi-national information campaign for all phases, designed to counter negative information operations. During this phase other possible threat actions could include construction site sabotage, vandalism, environmental contamination, staged accidents, and organized protest campaigns. Possible United States counteractions could include improved background checks, controlled site access measures, security protocols for workers, an aggressive CI program, two-man control for access to critical system components (hardware and software), incident tracking and analysis, and aggressive information/intelligence sharing between federal, state and local governments, as well as with United States allies.

The United States should initiate information operations that effectively portray the overwhelming positive aspects of a defensive missile shield both at home and abroad. Additional actions to counter an adversary's information campaign can include an increase in American science and technology efforts including, but not restricted to, enhanced cyber-attack countermeasures, an emphasis on National Information Infrastructure (NII) including EMP hardening of critical communication and data network sites, and development of multiple and redundant national telecommunication networks.

Within this phase the United States should undertake a comprehensive program to improve counterintelligence, surveillance, and protective measures. With regard to hardware and software in system development phases the United States should carefully determine the essential elements of information (EEI) regarding missile defense operation and couple them to protection measures in

the hardware and software acquisition process. To counter the continued vulnerability of commercial off the shelf (COTS) software to threat exploitation, industry and defense leaders should develop stringent guidelines to provide for the security of software throughout its life cycle. Consideration also should be given to utilizing MILSPEC software and hardware as an option to COTS. While this is an expensive option it may be necessary if commercial products continue to prove vulnerable to determined attacks.

Dedicated red teams can be employed to continuously evaluate critical missile system security (to include legacy components) and to recommend appropriate safeguards within these systems. Procurement activities for all systems and services should include enhanced, well-defined and measurable technical specifications for all systems and sub-components. Current technology must be improved and new technology developed to properly verify and validate the millions of lines of code required for various system components. National leaders must mandate that industry suppliers meet these new critical criteria for business practices, including defense contractor workforces (to include sub-contractors), in order to meet the physical and intellectual requirements of a new national missile defense program.

PHASE 2: System lOC Through Decision of Enemy to Engage in Hot War

In this phase potential adversaries will continue to conduct, and can be expected to expand, their campaign to deny the employment/deployment of United States missile defense systems. Continued covert attacks on both our NII and defensive missile industry must be anticipated. The United States should increase force protection measures related to IMD and industrial base assets. New and more direct programs to deny adversary access to the means of conducting their information campaign may be required. These means may include both technical and HUMINT solutions.

In a reversal of previous years' policies which have kept the press corps at arms length, it may now be necessary to actively seek out opportunities for providing positive, honest information about America's missile defense programs. Open, fair, and balanced reporting on American IMD programs should be tied to sustaining "the people's" understanding and backing of the systems development and deployment. This is critical to defeat an adversary's information campaign. Reporting successes, setbacks, and realistic capabilities may prove to be our strongest asset at home and abroad. There is an ever-increasing need for the United States to be able to nimbly adopt organizational and system changes to keep pace with technology changes.

PHASE 3: Hot War Through Conclusion of Conflict

During phase 3 the enemy could potentially conduct a synchronized, integrated, and sustained campaign against United States missile defenses designed to disable or suppress operations. Expected enemy actions could include: physical attack against critical command and control nodes, jamming and or physical destruction of both radar and long-haul communication networks, employment of anti-satellite weapons, activation of "Trojan horse" software, and direct attacks against elements of land and sea missile defenses. Attacks against critical space assets could result in the unintended escalation of hostilities, and suggest otherwise unwarranted defensive actions. Important to the

successful conclusion of hostilities is the development of detailed consequence management procedures. United States efforts to counter threats against IMD assets and the related infrastructure, both military and commercial, will ensure United States readiness to meet the challenges posed in the coming years.

CONCLUSIONS

Undoubtedly, weaknesses in the defense of IMD systems will increase with the proliferation of relatively low-cost missiles and the increasing sophistication of potential adversaries. To safeguard our missile defenses we must focus on integrated, layered network and physical defenses that weave together the full range of federal, state, and local assets in both public and industrial areas. Fully involved allies, strategically partnered in all facets of missile defense protection operations will measurably strengthen our overall efforts. While we remain concerned about physical attacks, we must also pay particular attention to political and information operations. The key to our ultimate success will be continuous research, development, testing, and evaluation of IMD defensive capabilities and procedures against the evolving multi spectrum capabilities of our adversaries.

This paper presents the issues and discussions developed by the working groups of the Defending The Defender - Keeping The Shield Strong Workshop. The Center for Strategic Leadership will continue to pursue the development and examination of these issues and conclusions through various workshops, symposia, and forums. We hope that the efforts of this workshop and future follow-on efforts will contribute to a significantly improved national security structure for the United States.

****

This and other CSL publications can be found online at http://carlisle-www.army.mil/usacsl/index.asp

****

U.S. ARMY WAR COLLEGE
Center for Strategic Leadership
650 Wright Avenue
Carlisle, PA 17013-5049

OFFICIAL BUSINESS

DEFENDING THE DEFENDER
KEEPING THE SHIELD STRONG